# *Groups Defined by the Orders of Two Generators and the Order of their Product.*

By G. A. Miller.

If the three numbers $l$, $m$, $n$ are the orders of three operators such that one of these operators is the product of the other two, it is known that the group generated by any two of these operators is completely defined by $l$, $m$, $n$, provided two of these numbers are equal to 2; or one is 2, the other 3 while the third is one of the three numbers 3, 4, 5.* In what follows we shall prove that these two operators may be so selected as to generate any one of an infinite system or groups of finite orders whenever $l$, $m$, $n$ do not satisfy one of the given conditions. In particular, if only the orders of two operators and that of their product are fixed, and if at least two of these orders exceed three, these operators can be so chosen as to generate any one of an infinite system of groups of a finite order. Hence two such operators generate a group of infinite order whenever they satisfy no conditions except such as depend upon their orders and the order of their product.

The method employed may be briefly described as follows: Since the order of a transitive substitution group of degree $n$ is a multiple of $n$ and a divisor of $n!$ this order is finite or infinite as $n$ is finite or infinite. If two substitutions of fixed orders can be so chosen that they generate a transitive substitution group whose degree is any multiple of a certain number, the order of such a group may have any one of an infinite number of values. Hence these substitutions can be so chosen as to generate any one of an infinite system of groups. The object is, therefore, to find two substitutions of the required orders such that their product is of the required order, and that they generate a transitive group whose degree is an arbitrary multiple of some number.

In what follows the three operators will be represented by $L$, $M$, $N$ and

* Bulletin of the American Mathematical Society, vol. VII, 1901, p. 424.

their orders by $l$, $m$, $n$ respectively. It will be assumed that $ML = N$ and that $l \leqq m \leqq n$, since these assumptions do not affect the generality of the results. The cases when $l = 2$ and when $l = 3$ will be considered separately, beginning with the former. The product of the following two substitutions

$$M_1 = a_1a_2a_3 \,.\, a_4a_5a_6 \,.\, a_7a_8a_9 \;\ldots\; a_{6k-2}a_{6k-1}a_{6k},$$
$$L_1 = a_3a_4 \,.\, a_5a_7 \,.\, a_6a_8 \,.\, a_9a_{10} \,.\, a_{11}a_{13} \,.\, a_{12}a_{14} \;\ldots\; a_{6k-3}a_{6k-2}$$

is composed of $k$ cycles of degree 6, where $k$ is any positive integer. In general, the product of the two substitutions

$$M_2 = a_1a_2a_3 \,.\, a_4a_5a_6 \,.\, a_7a_8a_9 \;\ldots\; a_{3\alpha k-2}a_{3\alpha k-1}a_{3\alpha k},$$
$$L_2 = a_3a_4 \,.\, a_6a_7 \;\ldots\; a_{3\alpha-3}a_{3\alpha-2} \,.\, a_{3\alpha-1}a_{3\alpha+1} \,.\, a_{3\alpha}a_{3\alpha+2} \;\ldots\; a_{3\alpha k-3}a_{3\alpha k-2}$$

is composed of $k$ cycles of degree $3\alpha$, $\alpha > 1$. Hence two substitutions of orders two and three respectively, whose product is an arbitrary multiple of three, can be so chosen as to generate any one of an infinite system of groups of finite order. When $\alpha > 3$, there are at least two letters which do not occur in $L_2$, in each of the cycles of degree $3\alpha$ mentioned above. By adding transpositions to $L_2$ each of these cycles can clearly be made of degree $3\alpha + 1$ or of degree $3\alpha + 2$ instead of $3\alpha$. When $\alpha = 3$, we may make the cycles of degree 10 by the same method. The remaining cases, i. e. when $n = 7$, 8 or 11 may be treated separately as follows, the substitutions being chosen in such a manner as to give the fundamental transitive group by omitting the last cycle of $M$ and the last two cycles of $L$. To obtain the generators of the transitive group whose degree is any multiple of the degree of this fundamental transitive group, it is only necessary to increase the subscripts of $L$ and $M$ by multiples of this degree.

$$M_3 = a_1a_2a_3 \,.\, a_4a_5a_6 \,.\, a_7a_8a_9 \,.\, a_{10}a_{11}a_{12} \,.\, a_{13}a_{14}a_{15} \,.\, a_{16}a_{17}a_{18} \,.\, a_{19}a_{20}a_{21} \,.\, a_{22}a_{23}a_{24} \,.\, a_{25}a_{26}a_{27} \,.$$
$$a_{28}a_{29}a_{30} \,.\, a_{31}a_{32}a_{33} \,.\, a_{34}a_{35}a_{36} \,.\, a_{37}a_{38}a_{39} \,.\, a_{40}a_{41}a_{42} \,.\, a_{43}a_{44}a_{45},$$
$$L_3 = a_3a_4 \,.\, a_5a_7 \,.\, a_6a_{10} \,.\, a_8a_{12} \,.\, a_{11}a_{13} \,.\, a_9a_{20} \,.\, a_{14}a_{16} \,.\, a_{15}a_{29} \,.\, a_{18}a_{29} \,.\, a_{21}a_{22} \,.\, a_{23}a_{25} \,.\, a_{24}a_{35} \,.$$
$$a_{26}a_{28} \,.\, a_{30}a_{31} \,.\, a_{32}a_{34} \,.\, a_{33}a_{38} \,.\, a_{36}a_{37} \,.\, a_{39}a_{40} \,.\, a_{41}a_{43} \,.\, a_{42}a_{44},$$
$$M_3L_3 = a_1a_2a_4a_7a_{12}a_6a_3 \,.\, a_5a_{10}a_{13}a_{16}a_{17}a_{19}a_9 \,.\, a_8a_{20}a_{22}a_{25}a_{28}a_{15}a_{11} \,.\, a_{14}a_{29}a_{31}a_{34}a_{24}a_{21}a_{18} \,.$$
$$a_{23}a_{35}a_{37}a_{33}a_{30}a_{26}a_{27} \,.\, a_{32}a_{38}a_{40}a_{43}a_{42}a_{39}a_{36} \,.\, a_{41}a_{44} \;\ldots,$$
$$M_4 = a_1a_2a_3 \,.\, a_4a_5a_6 \,.\, a_7a_8a_9 \,.\, a_{10}a_{11}a_{12} \,.\, a_{13}a_{14}a_{15} \,.\, a_{16}a_{17}a_{18} \,.\, a_{19}a_{20}a_{21} \,.\, a_{22}a_{23}a_{24} \,.\, a_{25}a_{26}a_{27},$$
$$L_4 = a_3a_4 \,.\, a_5a_7 \,.\, a_6a_{21} \,.\, a_8a_{19} \,.\, a_9a_{18} \,.\, a_{11}a_{15} \,.\, a_{12}a_{17} \,.\, a_{13}a_{22} \,.\, a_{14}a_{16} \,.\, a_{23}a_{25} \,.\, a_{24}a_{26},$$
$$M_4L_4 = a_1a_2a_4a_7a_{19}a_{20}a_6a_3 \,.\, a_5a_{21}a_8a_{18}a_{14}a_{11}a_{17}a_9 \,.\, a_{10}a_{15}a_{22}a_{25}a_{24}a_{13}a_{16}a_{12} \,.\, a_{23}a_{26} \;\ldots,$$
$$M_5 = a_1a_2a_3 \,.\, a_4a_5a_6 \,.\, a_7a_8a_9 \,.\, a_{10}a_{11}a_{12} \,.\, a_{13}a_{14}a_{15},$$
$$L_5 = a_3a_4 \,.\, a_5a_7 \,.\, a_6a_{10} \,.\, a_8a_9 \,.\, a_{11}a_{13} \,.\, a_{12}a_{14},$$
$$M_5L_5 = a_1a_2a_4a_7a_9a_5a_{10}a_{13}a_{12}a_6a_3 \,.\, a_{11}a_{14} \;\ldots$$

This completes the proof that there is an infinite number of groups for every value of $n > 5$ whenever $l = 2$ and $m = 3$. We proceed to the cases when $l = 2$ and $m = 4$. It is easy to see that the product of the following two substitutions is composed of $k$ cycles of degree 4:

$$M_6 = a_1a_2a_3a_4 \,.\, a_5a_6a_7a_8 \,\ldots\ldots\, a_{4k-3}a_{4k-2}a_{4k-1}a_{4k},$$
$$L_6 = a_3a_5 \,.\, a_4a_6 \,.\, a_7a_9 \,.\, a_8a_{10} \,\ldots\ldots\, a_{4k-5}a_{4k-3} \,.\, a_{4k-4}a_{4k-2}.$$

From this it follows that we may select $L$ in such a manner that $LM$ is of order $4\alpha$, and that $L$, $M$ generate a transitive group of degree $4\alpha k$, $\alpha$ and $k$ being arbitrary. To effect this, it is only necessary to select $L$ in such a manner as to connect some of the cycles of $M$ by a single transposition, while others are connected in the same manner as in $L_6$. When $\alpha > 2$, the order of the cycles of $N$ can be increased by three or less and diminished by at least one by means of additional transpositions in $L$. When $\alpha = 2$, the order of $N$ can clearly be increased by one or two in the same manner. It remains only to consider the cases when $n$ is one of the three members 5, 6, 7, The following substitutions prove the existence of an infinite number of groups in each of these cases:

$$N_7 \;= a_1a_2a_3a_4a_5 \,.\, a_6a_7a_8a_9a_{10} \,.\, a_{11}a_{12}a_{13}a_{14}a_{15},$$
$$L_7 \;= a_3a_6 \,.\, a_4a_8 \,.\, a_5a_7 \,.\, a_9a_{11} \,.\, a_{10}a_{12},$$
$$N_7L_7 = a_1a_2a_6a_5 \,.\, a_3a_8a_{11}a_{10} \,.\, a_4a_7 \,.\, a_9a_{12} \,\ldots\ldots$$
$$M_8 \;= a_1a_2a_3a_4 \,.\, a_5a_6a_7a_8 \,.\, a_9a_{10}a_{11}a_{12},$$
$$L_8 \;= a_3a_6 \,.\, a_4a_5 \,.\, a_7a_9 \,.\, a_8a_{10},$$
$$M_8L_8 = a_1a_2a_6a_9a_8a_4 \,.\, a_3a_5 \,.\, a_7a_{10} \,\ldots\ldots$$
$$M_9 \;= a_1a_2a_3a_4 \,.\, a_5a_6a_7a_8 \,.\, a_9a_{10}a_{11}a_{12} \,.\, a_{13}a_{14}a_{15}a_{16},$$
$$L_9 \;= a_3a_{10} \,.\, a_4a_6 \,.\, a_5a_9 \,.\, a_7a_\alpha \,.\, a_8a_\beta \,.\, a_{11}a_{13} \,.\, a_{12}a_{14},^*$$
$$M_9L_9 = a_1a_2a_{10}a_{13}a_{12}a_5a_4 \,.\, a_3a_6a_\alpha a_7a_\beta a_8a_9 \,.\, a_{11}a_{14} \,\ldots\ldots$$

From the two substitutions $M_6$, $L_6$ it follows directly that it is possible to select a substitution of order $m > 3$ and a substitution of order 2 so that the order of their product is an arbitrary multiple of $m$, and that they generate a transitive group whose degree is an arbitrary multiple of the order of their product. When $m > 6$, we can evidently make the order of this product any number $\gtreqless m$ by the addition of transpositions in $L$. Moreover, it is clear that

* Since two new elements are added by $L_9$, the remaining subscripts are obtained by increasing the given ones by 12 instead of by 14.

$n = 9$ is the only case which requires special considerations when $m = 6$. That there is also an infinity of groups in this case follows from the facts that there are substitutions of orders two and six whose product is of order 9,* and that there is an infinite number of groups when $l = 2$, $m = 3$, $n = 9$. When $m = 5$, there is also only one special case, viz. $n = 7$. The following two substitutions prove the existence of an infinite number of groups of finite order in this case:

$$M_{10} \quad = a_1a_2a_3a_4a_5 \, . \, a_6a_7a_8a_9a_{10} \, . \, a_{11}a_{12}a_{13}a_{14}a_{15} \, . \, a_{16}a_{17}a_{18}a_{19}a_{20} \, ,$$

$$L_{10} \quad = a_4a_{13} \, . \, a_5a_{11} \, . \, a_8a_9 \, . \, a_{10}a_{12} \, . \, a_{14}a_{16} \, . \, a_{15}a_{17} \, ,$$

$$M_{10}L_{10} = a_1a_2a_3a_{13}a_{16}a_{15}a_5 \, . \, a_4a_{11}a_{10}a_6a_7a_9a_{12} \, . \, a_{14}a_{17} \, \ldots .$$

This completes the consideration of all the cases when $l = 2$. Some additional cases may be reduced, in the following manner, to those which have been considered above. If a group is generated by two operators $(s_1, s_2)$, $s_1$ and all its transforms with respect to $s_2$ generate either the entire group or an invariant subgroup whose index under the entire group is a divisor of the order of $s_2$. In particular, if the order of $s_2$ is 2, $s_1$ and its transform with respect to $s_2$ generate either the entire group or a subgroup of half its order. In this special case, when $s_2^2 = 1$, the product of $s_1$ and $s_2^{-1}s_1s_2$ is $(s_1s_2)^2$. Hence, it follows from the preceding paragraphs that two operators of the same order $> 2$ whose product is also of a higher order than 2, can always be so selected that they generate any one of an infinite system of groups. For instance, from the fact that two operators of orders 2 and 5 respectively, whose product is of order 8, can be so selected as to generate any one of an infinite system of groups of finite order, it follows that two operators of order 5 whose product is of order 4 have the same property. Since the group generated by two given operators is identical with the one generated by one of these operators and the product of the operators, it remains only to consider the cases when no two of the numbers $l$, $m$, $n$ have a common factor $> 2$ and when $l > 2$.

When $l = 3$ and $m = 4$, we need to consider only one value of $n$, viz. 5, since in all the other cases it has been proved that $M$ can be replaced in part by an operator of order two, which can be so selected that any one of some infinite system of groups is generated by $L$ and $M$. The following substitutions prove

---

* American Journal of Mathematics, vol. XXII, 1900, p. 185.

that this special case does not present an exception to the general theorem under consideration:

$$M_{11} = a_1a_2a_3a_4 . a_5a_6a_7a_8 . a_9a_{10}a_{11}a_{12}, \quad L_{11} = a_4a_5a_6 . a_7a_9a_\alpha . a_8a_{11}a_\beta,$$
$$M_{11}L_{11} = a_1a_2a_3a_5a_4 . a_6a_9a_{10}a_\beta a_8 . a_7a_{11} \ldots . \text{*}$$

When $l = 3$ and $m = 5$, we may assume that $n$ is odd, for if it were divisible by 4 or contained either 3 or 5 as a factor, it would come under the preceding cases. Hence it must contain some odd factor greater than 5. It is now clear that it may be assumed that both $m$ and $n$ are odd whenever $m > 4$. Since the product of the two substitutions $a_1a_2a_3a_4a_5 . a_6a_7a_8a_9a_{10} . a_{11}a_{12}a_{13}a_{14}a_{15} \ldots . a_l$ and $a_5a_6a_7 . a_{10}a_{11}a_{12} \ldots . a_la_1a_2$ is of order five and involves an arbitrary multiple of 5 letters, and since $a_1a_2a_3a_4a_5 . a_6a_7a_8a_9a_{10}$ into $a_5a_6a_\alpha$ is a cyclic substitution of degree 11, it is evident that when $l = 3$ and $m > 4$, $L$ and $M$ can be so chosen as to generate a transitive group whose degree is any multiple of a fixed number.†

It may now be assumed that each of the three numbers $l$, $m$, $n$ is odd and exceeds 3. The method employed in the preceding paragraph requires only slight modification to apply to all of these cases. It is based upon the following two propositions: 1). In combining two cycles, any odd number ($< l - 1$) of letters may be added; e. g. $a_1a_2a_3a_4a_5a_6a_7 . a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}$ into $a_7a_8a_\alpha a_\beta a_\gamma$ and into $a_7a_8a_9a_{10}a_\alpha$ gives substitutions of order 17 and 15 respectively. 2). In closing a cycle, any even number ($< l - 2$) of letters may be added; e. g. $a_1a_2a_3a_4a_5a_6a_7 . a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}$ into $a_7a_8a_\alpha a_\beta a_9 . a_{14}a_1a_{\alpha_1}a_{\beta_1}a_2$ and into $a_7a_8a_{10}a_{11}a_9 . a_{14}a_7a_3a_4a_2$ gives substitutions of orders 9 and 7 respectively, each of which is composed of two cycles. These propositions combined with the fact that the order of $N$ can be increased by any even number $< m$ by means of additional cycles in $L$ complete the proof of the required theorem, viz. *If two of the three numbers $l$, $m$, $n$ are equal to 2 or if $l = 2$, $m = 3$, and $n = 3$, 4, or 5, the group generated by $L$ and $M$ is completely defined by the values $l$, $m$, $n$. For all other sets of values of $l$, $m$, $n$ any two of the substitutions $L$, $M$, $N$ can be so constructed as to generate any one of some infinite system of groups of finite order.*

ITHACA, N. Y., *August*, 1901.

---

* The fundamental transitive group is of degree 10 and the subscripts are increased by multiples of 8 to obtain the other transitive groups. To obtain a definite transitive group, the last cycle of $L$ is to be changed so as to contain two letters not found in $M$.

† C. f. American Journal, l. c.